

**METHOD AND APPARATUS FOR GRAPH-BASED PARTITION
OF CRYPTOGRAPHIC FUNCTIONALITY**

Abstract

5 Techniques are disclosed for partitioning of cryptographic functionality, such as authentication code verification or generation ability, so as to permit delegation of at least one of a number of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. The cryptographic functionality is characterizable as a graph comprising a plurality of nodes, and a given set of the nodes is associated with a corresponding
10 one of the distinct portions of the cryptographic functionality. Information representative of one or more of the nodes is transmitted from the delegating device to the recipient device such that the recipient device is thereby configurable for authorized execution of a corresponding one of the distinct portions of the cryptographic functionality. Advantageously, the invention provides a particularly efficient mechanism for the provision of cryptographic functionality in accordance
15 with a subscription model.